

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-067268

(43)Date of publication of application : 16.03.2001

(51)Int.Cl.

G06F 12/14

H04L 9/36

H04N 7/16

(21)Application number : 11-237274

(71)Applicant : TOSHIBA CORP

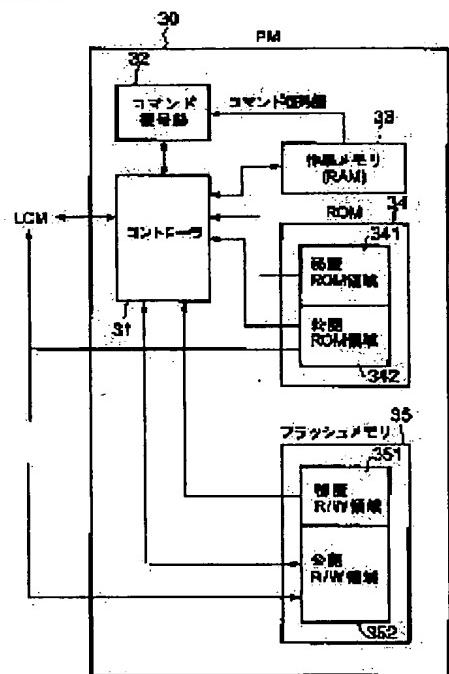
(22)Date of filing : 24.08.1999

(72)Inventor : KAMIBAYASHI TATSU  
TAMURA MASABUMI

## (54) METHOD FOR MANAGING CONTENTS, AND STORAGE MEDIUM

(57)Abstract:

**PROBLEM TO BE SOLVED:** To make preventable the failure of security due to the alteration of a secret region operation command.  
**SOLUTION:** At the time of issuing a desired secret region operation command from an LCM to be realized on a PC for operating a secret R/W region 351 ensured so that its boundary can be brought into contact with a public R/W region 352 on a memory 35, the whole command or the parameter part of the command is enciphered, and the enciphered secret region operation command is transmitted to a PM 30 side. At the time of receiving the secret region operation command, a controller 31 of the PM 30 allows a command decoding part 32 to decode the whole command or the parameter part of the command, and the secret R/W region 351 is operated according to the decoded secret region operation command. In this case, when the command is a CHANGE command for changing the secret R/W region 351, the controller 31 deletes the data of the reduced/enlarged part of the secret R/W region 351 at the time of changing the secret R/W region 351.



(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-67268

(P2001-67268A)

(43)公開日 平成13年3月16日(2001.3.16)

(51) Int.Cl.<sup>7</sup>  
 G 06 F 12/14  
 H 04 L 9/36  
 H 04 N 7/16

識別記号  
3 2 0

F I  
 G 06 F 12/14  
 H 04 N 7/16  
 H 04 L 9/00

テマコード(参考)  
3 2 0 B 5 B 0 1 7  
Z 5 C 0 6 4  
6 8 5 5 J 1 0 4

審査請求 未請求 請求項の数 5 O.L. (全 10 頁)

(21)出願番号 特願平11-237274  
 (22)出願日 平成11年8月24日(1999.8.24)

(71)出願人 000003078  
 株式会社東芝  
 神奈川県川崎市幸区坂川町72番地  
 (72)発明者 上林 達  
 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内  
 (72)発明者 田村 正文  
 東京都港区芝浦一丁目1番1号 株式会社東芝本社事務所内  
 (74)代理人 100058479  
 弁理士 鈴江 武彦 (外6名)

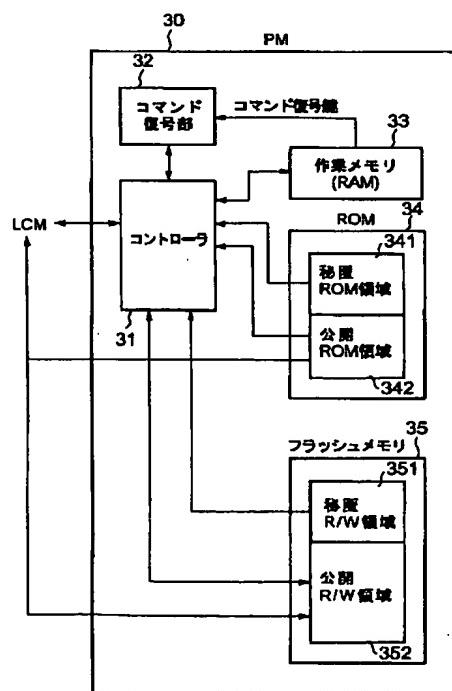
最終頁に続く

## (54)【発明の名称】 コンテンツ管理方法及び記憶媒体

## (57)【要約】

【課題】秘匿領域操作コマンドの改ざんによるセキュリティの破綻を防ぐ。

【解決手段】メモリ35上に公開R/W領域352と境界を接するように確保された秘匿R/W領域351を操作するために、PC上に実現されるLCMから所望の秘匿領域操作コマンドを発行する際には、コマンド全体または当該コマンドのパラメータ部分を暗号化し、その暗号化された秘匿領域操作コマンドをPM30側に送る。PM30のコントローラ31は、この秘匿領域操作コマンドを受け取った場合、コマンド復号部32により、当該コマンドのコマンド全体またはパラメータ部分を復号させ、この復号された秘匿領域操作コマンドに従って秘匿R/W領域351を操作する。ここで、上記コマンドが秘匿R/W領域351を変更するCHANGEコマンドの場合、コントローラ31はその領域変更に際し、秘匿R/W領域351の縮小/拡大部分のデータを消去する。



## 【特許請求の範囲】

【請求項1】 デジタル・コンテンツが記録される記憶媒体に確保された、当該コンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される、特定手続にてのみアクセスが可能な秘匿領域を、専用のコマンドである秘匿領域操作コマンドによって操作するコンテンツ管理方法であって、

前記記憶媒体に対する所望のタイプの秘匿領域操作コマンドを発行するに際し、当該コマンド全体または当該コマンドのパラメータ部分を暗号化し、

前記記憶媒体側では、前記コマンド全体またはパラメータ部分が暗号化された秘匿領域操作コマンドを受け取った場合、当該コマンドのコマンド全体またはパラメータ部分を復号し、

この復号された秘匿領域操作コマンドに従って前記秘匿領域を操作することを特徴とするコンテンツ管理方法。

【請求項2】 記憶媒体上の所定のメモリ領域を分割することにより、デジタル・コンテンツが記録される、通常手続でアクセスが可能な公開領域と境界を接して確保された、前記コンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される、特定手続にてのみアクセスが可能な秘匿領域を、専用のコマンドである秘匿領域操作コマンドによって操作するコンテンツ管理方法であって、

前記記憶媒体に対する所望のタイプの秘匿領域操作コマンドを発行するに際し、当該コマンド全体または当該コマンドのパラメータ部分を暗号化し、

前記記憶媒体側では、前記コマンド全体またはパラメータ部分が暗号化された秘匿領域操作コマンドを受け取った場合、当該コマンドのコマンド全体またはパラメータ部分を復号し、

この復号された秘匿領域操作コマンドに従って前記秘匿領域を操作し、当該コマンドが前記秘匿領域のサイズの変更を指示する特定秘匿領域操作コマンドの場合には、前記秘匿領域と前記公開領域との境界を移動することで前記秘匿領域のサイズを変更し、少なくとも前記秘匿領域が縮小変更される場合は、その秘匿領域変更に際してその変更部分のデータを消去することを特徴とするコンテンツ管理方法。

【請求項3】 デジタル・コンテンツが記録される記憶媒体に確保された、当該コンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される、特定手続にてのみアクセスが可能な秘匿領域を、専用のコマンドである秘匿領域操作コマンドによって操作するコンテンツ管理装置であって、

前記記憶媒体に対する所望のタイプの秘匿領域操作コマンドを発行するに際し、当該コマンド全体または当該コマンドのパラメータ部分を暗号化するコマンド暗号化手段と、

前記コマンド暗号化手段により前記コマンド全体または

パラメータ部分が暗号化された秘匿領域操作コマンドを前記記憶媒体側に送信する送信手段とを具備することを特徴とするコンテンツ管理装置。

【請求項4】 デジタル・コンテンツが記録される記憶媒体において、前記記憶媒体に記録されたコンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される、特定手続にてのみアクセスが可能な秘匿領域が確保されるメモリと、

10 前記秘匿領域を操作するための専用のコマンドであり、そのコマンド全体または当該コマンドのパラメータ部分が暗号化された秘匿領域操作コマンドを受け取った場合に、この暗号化された秘匿領域操作コマンドのコマンド全体またはパラメータ部分を復号するコマンド復号手段と、

前記コマンド復号手段により復号された秘匿領域操作コマンドに従って前記秘匿領域を操作するコントローラとを具備することを特徴とする記憶媒体。

【請求項5】 デジタル・コンテンツが記録される、通常手続でアクセスが可能な公開領域と、前記公開領域に記録されたコンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される、特定手続にてのみアクセスが可能な秘匿領域とが境界を接して確保されたメモリと、

前記秘匿領域を操作するための専用のコマンドであり、そのコマンド全体または当該コマンドのパラメータ部分が暗号化された秘匿領域操作コマンドを受け取った場合に、この暗号化された秘匿領域操作コマンドのコマンド全体またはパラメータ部分を復号するコマンド復号手段と、

前記コマンド復号手段により復号された秘匿領域操作コマンドに従って前記秘匿領域を操作するコントローラであって、当該コマンドが前記秘匿領域のサイズの変更を指示する特定秘匿領域操作コマンドの場合には、前記秘匿領域と前記公開領域との境界を移動することで前記秘匿領域のサイズを変更し、少なくとも前記秘匿領域が縮小変更される場合は、その秘匿領域変更に際してその変更部分のデータを消去するコントローラとを具備することを特徴とする記憶媒体。

40 【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、画像データや音楽データに代表される種々のデジタル・コンテンツの著作権保護を図るために好適なコンテンツ管理方法及び記憶媒体に関する。

【0002】

【従来の技術】 近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレーヤー、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メ

ィアに格納された画像データや音楽データなど様々なデジタル・コンテンツを再生できるほか、インターネット等を通じてデジタル・コンテンツをダウンロードして使用することもできる。

【0003】これらのデジタル・コンテンツは、例えばMPEG2、MP3といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタル・コンテンツを不正使用から保護するための技術の必要性が叫ばれている。特に、メモリカードのように別の機器に移動しても記録／再生できるリムーバブルな記憶媒体は、その仕様が基本的にはオープンであり、コンテンツの移動／コピーを自由に行うことができるので、その記憶媒体に記憶されたコンテンツを不正なコピー／移動から保護できるようにすることは重要である。

【0004】そこで、メモリカードのように記憶メディア部とコントローラとが一体化された記憶媒体については、秘匿された特定手続にてのみアクセスでき、ユーザからはアクセスできないアクセス不能領域（秘匿領域）を設け、そこにコピー制御情報、移動制御情報などの、コンテンツの使用に必要な重要な情報を格納しておくことにより、コンテンツの保護を図ることが考えられる。ここでは、パソコンコンピュータ、セットトップボックス、プレーヤーなどの電子機器と記憶媒体の間でコンテンツのコピー／移動を行う際に、それぞれが、著作権保護（コンテンツ保護）に関する所定の仕組み（つまり所定のコンテンツ保護機能）を共有している正当なものであるかを相互に認証し、正しいと認証できた場合に相互に共有する鍵生成のアルゴリズムに従って鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキー（コンテンツを復号するためのコンテンツ復号鍵）の暗号化／復号化またはコンテンツの暗号化／復号化に用いることが考えられている。

#### 【0005】

【発明が解決しようとする課題】さて、デジタル・コンテンツを利用するアプリケーションを搭載した機器（以下、ホストと称する）では、上述の著作権保護の観点から、記憶媒体（メモリカード等の記憶メディア部とコントローラとが一体化された記憶媒体）の秘匿領域に格納されているコンテンツキー（コンテンツ復号鍵）などを、確実に上書きしたり消去したりすることが必要となる。

【0006】ところが従来の記憶媒体の秘匿領域に対する書き込みや消去のコマンド（秘匿領域操作コマンド）には、そのコマンド全体、或いはそのコマンドのパラメータの改ざんに対して何ら考慮されていなかった。このため、ホストと記憶媒体との間の通信を傍受してコマンドを改ざんし、記憶媒体の秘匿領域に格納されている特定のデータの消去を阻害するなど、セキュリティに対す

る攻撃が存在する虞がある。

【0007】本発明は上記事情を考慮してなされたものでその目的は、秘匿領域を対象とする操作を指示するコマンド（秘匿領域操作コマンド）の改ざんによるセキュリティの破綻を防ぐことができるコンテンツ管理方法及び記憶媒体を提供することにある。

#### 【0008】

【課題を解決するための手段】本発明は、デジタル・コンテンツが記録される記憶媒体に確保された、当該コンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される秘匿領域を操作するために、所望のタイプの秘匿領域操作コマンドを発行するに際し、当該コマンド全体または当該コマンドのパラメータ部分を暗号化して、かかる後に、この暗号化された秘匿領域操作コマンドを記憶媒体側に送るようとする一方、記憶媒体側では、コマンド全体またはパラメータ部分が暗号化された秘匿領域操作コマンドを受け取った場合、当該コマンドのコマンド全体またはパラメータ部分を復号し、この復号された秘匿領域操作コマンドに従って秘匿領域を操作することを特徴とする。ここで、秘匿領域操作コマンドのコマンド全体またはパラメータ部分の暗号化に用いる暗号鍵と、秘匿領域操作コマンドの暗号化されたコマンド全体または暗号化されたパラメータ部分の復号に用いる復号鍵とは、暗号化側と復号化側との間の通信を通じて、相互に共有する鍵生成のアルゴリズムに従い生成すればよい。また、この鍵生成は、秘匿領域操作コマンドの送信の都度、その送信に先立って行われるようにするといよ。

【0009】このように、記憶媒体のメモリ領域に確保された秘匿領域を対象とする秘匿領域操作コマンドのコマンド全体またはパラメータ部分を暗号化して当該記憶媒体に送り、当該記憶媒体ではそれを復号化して実行することで、コマンド改ざんにより秘匿領域の特定のデータの消去が阻害されるといった、セキュリティの破綻を防ぐことができる。

【0010】ここで、秘匿領域操作コマンド全体を暗号化した場合には、そのパラメータ部分で指定されるメモリ領域上の位置や操作の対象となるサイズを改ざんすることが極めて困難となるだけでなく、コマンドの同定すら困難となる。一方、秘匿領域操作コマンドのパラメータ部分だけを暗号化した場合には、OPコード部分は暗号化されていないため、記憶媒体側では秘匿領域操作コマンドを受信した際に、直ちに当該コマンドの解釈処理に入ることができるため、パラメータ部分で指定されるメモリ領域上の位置や操作の対象となるサイズを改ざんすることを防止しながら、記憶媒体側での動作（処理の割当て）の最適化を図ることができる。

【0011】また本発明は、上記記憶媒体上の所定のメモリ領域を分割して、デジタル・コンテンツが記録される、通常手続でアクセスが可能な公開領域と、上記の秘

匿領域と、境界を接するようにして確保する一方、上記秘匿領域操作コマンドの1つとして、秘匿領域のサイズの変更指示が可能な特定秘匿領域操作コマンド（CHANGEコマンド）が利用可能なようにし、記憶媒体側で復号された秘匿領域操作コマンドが特定秘匿領域操作コマンドの場合には、秘匿領域と公開領域との境界を移動することで秘匿領域のサイズを変更し、少なくとも秘匿領域が縮小変更される場合は、その秘匿領域変更に際してその変更部分のデータを消去するようにしたことをも特徴とする。

【0012】本発明においては、秘匿領域操作コマンドの改ざんを防ぎながら、当該コマンドとして特定秘匿領域操作コマンドを使用した場合には、秘匿領域と公開領域とのサイズの比率を変更すること、即ち秘匿領域を縮小すると共にその縮小分だけ公開領域を拡大すること、或いは秘匿領域を拡大すると共にその拡大分だけ公開領域を縮小することができる。これにより記憶媒体を、例えば、1コンテンツ当たりのデータサイズが大きくなるビデオデータの記憶に用いるような場合には、扱える総コンテンツサイズを重視して秘匿領域を縮小すると共に公開領域を拡大し、1コンテンツ当たりのデータサイズが小さくて済む音楽データの記憶に用いる場合には、扱える総コンテンツ数を重視して秘匿領域を拡大すると共に公開領域を縮小するといったことが可能となる。

【0013】しかも本発明においては、少なくとも秘匿領域が縮小変更される場合は、その秘匿領域変更に際してその変更部分のデータ、即ち秘匿領域と公開領域との現在の境界（変更前の境界）と変更後の境界との間のデータが自動的に消去されることから、秘匿領域の縮小変更に伴ってその秘匿領域の縮小部分が公開領域に加えられたとしても、その縮小部分に記憶されていた秘密のデータが漏洩する虞はない。ここで、秘匿領域が拡大変更される場合にも、その変更部分のデータが自動的に消去されるようになるとよい。この場合、公開領域のうち、秘匿領域との境界の領域部分に所望のデータを書き込んだ後、秘匿領域操作コマンドを用いて当該領域部分が秘匿領域側に入るように秘匿領域を拡大変更することで、その拡大部分の本来秘匿されるべきデータを自由に利用可能にしようとする「攻撃」がなされても、対抗できる。

#### 【0014】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図1は本発明の一実施形態に係るコンテンツ利用管理システムの構成を主として示すブロック図である。

【0015】コンテンツ利用管理システム（以下、LCM（Licence（SDMI-）Compliant Module）と称する）10は、メモリカード等の記憶メディア（以下、PM（Portable Memory）と称する）30に記録できる複製コンテンツの数を規制し、当該PM30に記録された複製コ

ンテンツの記録、再生等を行うもので、例えば、パーソナルコンピュータ（以下、PCと称する）1上で実行可能なソフトウェアとして実現されている。

【0016】LCM10は、コンテンツ配信サーバ等から配信される暗号化コンテンツまたはそのライセンス（利用条件と暗号化コンテンツの復号鍵）などを受信する機能を有する。

【0017】LCM10は、当該LCM10の中核をなすセキュア・コンテンツ・サーバ11を有している。セ

10 キュア・コンテンツ・サーバ11は、LCM10で受信される、利用者が購入した暗号化コンテンツを図示せぬデータ格納部に格納し、その復号鍵（コンテンツ復号キー）を図示せぬライセンス格納部に格納する。なお、受信された暗号化コンテンツは、一旦復号され、かかる後に形式変換や再暗号化が施されることが多い。このセキュア・コンテンツ・サーバ11が管理するコンテンツは、当該サーバ11によりLCM10上で再生することも可能である。

【0018】セキュア・コンテンツ・サーバ11はまた、メディアI/F部13に装着可能なPM30に対してコンテンツデータ（デジタル・コンテンツ）を当該I/F部13経由で出力する機能を有している。このPM30は、専用の記録再生装置（以下、簡単にPD（Portable Device）と称する）20にセットして用いることで、当該PM30に記録されたコンテンツをPD20上で再生することもできる。セキュア・コンテンツ・サーバ11は、PD20にセットされたPM30に対し、PD I/F部12及びPD20経由で出力する機能も有する。つまり、セキュア・コンテンツ・サーバ11から

30 PM30へのコンテンツの記録は、メディアI/F部13を通じて直接行われるか、またはPD I/F部12及びPD20を経由して行われる。

【0019】I/F部12、13は、それぞれセキュア・コンテンツ・サーバ11から当該I/F部12、13を介してPM30側に送られる特定コマンドである秘匿R/W領域操作コマンド（後述する秘匿R/W領域351を対象とする操作を指示するコマンド）を暗号化するコマンド暗号化部120、130を有している。

【0020】セキュア・コンテンツ・サーバ11は更に、PC1の入出力装置（図示せず）からの入力を受け付けるユーザI/F部14を有している。ユーザがキーボード、マウス等の入力装置を操作して入力した指示は、このユーザI/F部14で受け付けられてセキュア・コンテンツ・サーバ11に渡される。この指示には、後述する秘匿R/W領域351の大きさの変更指示も含まれる。

【0021】図2は、PM30の構成を示す。同図に示すように、PM30は、LCM10から直接にまたはPD20を介して送られるコマンドを解釈・実行するコントローラ31と、暗号化されたコマンドを復号するコマ

ンド復号部32と、コントローラ31とコマンド復号部32によってのみアクセスが可能な、例えばRAMにより構成される作業メモリ33と、読み出し専用の不揮発性メモリとしてのROM34と、書き換え可能な不揮発性メモリとしてのフラッシュメモリ35とを備えている。

【0022】ROM34の記憶領域は、コントローラ31を通して非公開の手順（つまり秘匿された特定手続）でしかアクセスできない読み出し専用の記憶領域（以下、秘匿ROM領域と称する）341と、通常の手順にてアクセス可能な読み出し専用の記憶領域（以下、公開ROM領域と称する）342とに割り当てられている。

【0023】秘匿ROM領域341には、対応するPM30に固有の秘密情報である秘匿メディアID等の定数が予め記憶される。一方、公開ROM領域342には、対応するPM30の識別情報としてのメディアID、デジタル・コンテンツの記録または再生のためのアクセス要求を無効化すべき機器（LCM、PD）を表す情報等が記憶される。

【0024】次に、フラッシュメモリ35の記憶領域は、コントローラ31を通して非公開の手順でしかアクセスできない記憶領域（以下、秘匿R/W領域と称する）351と、通常の手順にてアクセス可能な記憶領域（以下、公開R/W領域と称する）352とに割り当てられている。

【0025】公開R/W領域352には、暗号化されたコンテンツ・データ（暗号化コンテンツ）が記憶される。一方、秘匿R/W領域351には、公開R/W領域352に記憶されるコンテンツ・データに対応する、当該コンテンツ・データを復号するためのコンテンツキー（コンテンツ復号鍵）が記憶される。秘匿R/W領域351にはまた、当該秘匿R/W領域351の開始アドレスとサイズの情報が記憶される。この情報は、秘匿R/W領域351の終了アドレス側の所定位置に記憶される。ここで用いられるアドレスは、特に断らない限り、メモリの物理アドレスではなくて、そのメモリが割り当てられるアドレス空間のアドレスを表す。

【0026】図3は、フラッシュメモリ35の記憶領域のメモリマップの一例を示す。同図に示すように、本実施形態では、秘匿R/W領域351はフラッシュメモリ35の記憶領域の高アドレス側に割り当てられ、公開R/W領域352は同じく低アドレス側に割り当てられている。ここで、秘匿R/W領域351の終了アドレスはフラッシュメモリ35の最終物理アドレスが割り当てられるメモリアドレス空間のアドレスに一致し、公開R/W領域352の開始アドレスはフラッシュメモリ35の先頭物理アドレス（0番地）が割り当てられるメモリアドレス空間のアドレスに一致する。また、秘匿R/W領域351の開始アドレスは、公開R/W領域352の終了アドレスに一致する。本実施形態では、この秘匿R/

W領域351の開始アドレス（=公開R/W領域352の終了アドレス）、つまり秘匿R/W領域351と公開R/W領域352との境界を、ユーザの指示に応じてLCM10側から発行されるCHANGEコマンド（秘匿R/W領域変更命令）と呼ぶ専用のコマンド（命令）の実行により指定サイズだけ可変できるようになっている。

【0027】図4は、LCM10からPM30に対して発行される秘匿R/W領域操作コマンド（秘匿領域操作コマンド）の形式を示す。

【0028】ここでは、各秘匿R/W領域操作コマンド（コマンドデータ）は、SENDと呼ばれる送信命令でPM30側に送られる。このコマンドデータは、先頭から順に、秘匿R/W領域操作の種別、つまりコマンド種別を示すコマンドコードとしてのOPコードと、秘匿R/W領域操作の対象となる記憶領域（秘匿R/W領域351内の領域）の開始位置のアドレス空間上のアドレス（開始アドレス）を示すADDRESSと、秘匿R/W領域操作の対象となる領域サイズを例えばバイト単位で示すLENGTHとから構成される。本実施形態において、OPコードは1バイト、ADDRESSは4バイト、そしてLENGTHは2バイトで、それぞれ表現される。コマンドデータのうち、OPコードを除くデータを、オペランド或いはパラメータと呼ぶ。また、本実施形態で適用される秘匿R/W領域操作コマンドには、前記したCHANGEコマンド（秘匿R/W領域変更命令）の他に、秘匿R/W領域351の指定領域からのデータ読み出しを指示するREADコマンド（秘匿R/W領域読み出し命令）、秘匿R/W領域351の指定領域へのデータ書き込みを指示するWRITEコマンド（秘匿R/W領域書き込み命令）、秘匿R/W領域351内の指定領域のデータ消去を指示するERASEコマンド（秘匿R/W領域消去命令）がある。

【0029】次に、本実施形態の動作を、図5乃至図7のフローチャートを参照して説明する。まず、LCM10のセキュア・コンテンツ・サーバ11からメディアI/F部13（またはPD1/F部12）に対して、PM30への秘匿R/W領域操作コマンドの送信が要求され、対応するコマンドデータが渡されたものとする。すると、I/F部13（または12）は、セキュア・コンテンツ・サーバ11から渡されたコマンドデータ全体、つまりOPコード（1バイト）、ADDRESS（4バイト）、及びLENGTH（2バイト）の合計7バイトのコマンドデータを、LCM10が有するコマンド暗号化鍵を用いてコマンド暗号化部130（または120）により暗号化し、その暗号化されたコマンドデータをSEND命令により、そのまま（またはPD20を介して）PM30のコントローラ31に送信する（ステップS1）。

【0030】PM30内のコントローラ31は、LCM

10側から送られた暗号化コマンドを受け取ると、その暗号化コマンドをコマンド復号部32に渡して、復号を要求する（ステップS2）。

【0031】するとコマンド復号部32は、コントローラ31から渡された暗号化コマンドを、当該コマンドの暗号化に用いられたコマンド暗号鍵に対応して生成されたコマンド復号鍵で復号する（ステップS3）。このコマンド復号鍵は、例えば、対応する秘匿R/W領域操作

コマンドの送信に先立って行われる、LCM10とPM30のコントローラ31との間の通信を通じて、相互に共有する鍵生成のアルゴリズムに従いコントローラ31により生成される。生成されたコマンド復号鍵はPM30の作業メモリ33に格納される。一方、このコマンド復号鍵に対応するコマンド暗号鍵は、LCM10のセキュア・コンテンツ・サーバ11にて生成される。

【0032】コマンド復号部32は、暗号化コマンドを復号すると、その復号されたコマンド、つまり平文のコマンドをコントローラ31に返す（ステップS4）。これによりコントローラ31は、コマンド復号部32から返されたコマンド（復号された秘匿R/W領域操作コマンド）のOPコードを解釈して、そのコマンド種別（命令種別）を判断する（ステップS5）。

【0033】もし、OPコードがREADコマンド（秘匿R/W領域読み出し命令）を指定しているならば（ステップS6）、コントローラ31は当該READコマンドのパラメータ（オペランド）ADDRESS, LENGTHに従って、ADDRESSで指定される秘匿R/W領域351の位置からLENGTHバイトのデータを読み出し（ステップS7）、その読み出したデータをLCM10に転送して動作（READコマンドの実行）を終了する（ステップS8）。

【0034】また、OPコードがWRITEコマンド（秘匿R/W領域書き込み命令）を指定しているならば（ステップS9）、コントローラ31は当該WRITEコマンドのパラメータADDRESS（アドレス）、LENGTH（データ長）を作業メモリ33に一旦格納する（ステップS10）。このステップS10の処理により、WRITEコマンドに続いてLCM10側から転送される書き込みデータの格納先（の開始位置）とデータ長を示す情報が作業メモリ33に保持される。

【0035】コントローラ31は、ステップS10を実行すると、LCM10から転送される書き込みデータを受け取る（ステップS11）。そしてLCM10は、受け取った書き込みデータを、先のステップS10で作業メモリ33に格納したWRITEコマンドのパラメータADDRESS, LENGTHに従って、ADDRESSで指定される秘匿R/W領域351の位置からLENGTHバイトだけ書き込んで動作（WRITEコマンドの実行）を終了する（ステップS12）。

【0036】また、OPコードがERASEコマンド

（消去命令）を指定しているならば（ステップS13）、コントローラ31は当該ERASEコマンドのパラメータADDRESS, LENGTHに従って、ADDRESSで指定される秘匿R/W領域351の位置からLENGTHで指定されるデータ長（バイト長）だけ、該当するデータを消去して動作（ERASEコマンドの実行）を終了する（ステップS14）。ここでデータ消去は、該当する領域に、所定のデータ、例えば0を書き込むことにより、つまり該当する領域のデータを0で置換することにより行われる。

【0037】また、OPコードがCHANGEコマンド（秘匿R/W領域変更命令）を指定しているならば（ステップS15）、コントローラ31は当該CHANGEコマンド中のADDRESS（つまり変更指定された秘匿R/W領域351の開始アドレス）と、秘匿R/W領域351の所定位置に記憶されている当該秘匿R/W領域351の開始アドレス（つまり現在の秘匿R/W領域351の開始アドレス）とを比較することで、秘匿R/W領域351の縮小が指定されているのか否か（つまり拡大が指定されているのか）を判定する（ステップS16）。

【0038】もし、秘匿R/W領域351の指定開始アドレスが現開始アドレスより大きいならば、コントローラ31は秘匿R/W領域351の縮小が指定されていると判定し、フラッシュメモリ35の現開始アドレスからCHANGEコマンド中のLENGTHの示すデータ長だけ（つまり上記指定開始アドレスまで）該当するデータを消去する（ステップS17）。そしてコントローラ31は、秘匿R/W領域351の開始位置（秘匿R/W領域351と公開R/W領域352との境界位置）をCHANGEコマンド中のADDRESSの指定する位置に変更して、当該秘匿R/W領域351をCHANGEコマンド中のLENGTHの指定するサイズだけ縮小すると同時に、同サイズだけ公開R/W領域352を拡大し、動作（CHANGEコマンドの実行）を終了する（ステップS18）。このステップS18の処理は、秘匿R/W領域351の終了アドレス側の所定位置に格納されている、当該秘匿R/W領域351の開始アドレスとサイズの情報を、当該秘匿R/W領域351の縮小後の情報を書き換えることで実現される。

【0039】これに対し、秘匿R/W領域351の指定開始アドレスが現開始アドレスより小さいならば、コントローラ31は秘匿R/W領域351の拡大が指定されていると判定し、フラッシュメモリ35の上記指定開始アドレス（CHANGEコマンド中のADDRESSで指定されるフラッシュメモリ35のアドレス）から当該CHANGEコマンド中のLENGTHの示すデータ長だけ（つまり上記現開始アドレスまで）該当するデータを消去する（ステップS19）。そしてコントローラ31は、秘匿R/W領域351の開始位置をCHANGE

コマンド中のADDRESSESの指定する位置に変更して、当該秘匿R/W領域351をCHANGEコマンド中のLENGTHの指定するサイズだけ拡大すると同時に、同サイズだけ公開R/W領域352を縮小し、動作(CHANGEコマンドの実行)を終了する(ステップS20)。このステップS20の処理は、秘匿R/W領域351の終了アドレス側の所定位置に格納されている、当該秘匿R/W領域351の開始アドレスとサイズの情報を、当該秘匿R/W領域351の拡大後の情報を書き換えることで実現される。

【0040】図8に、秘匿R/W領域351の開始アドレスがAD1の状態で、CHANGEコマンドによりAD2(但し、AD2>AD1)に変更することが指定された場合の、当該CHANGEコマンド実行後のフラッシュメモリ35のメモリマップを示す。ここでは、フラッシュメモリ35内のAD1～AD2までの領域353のデータが上記ステップS17にて消去される。そして、この領域353の分だけ、秘匿R/W領域351は縮小され、公開R/W領域352は拡大される。

【0041】以上、秘匿R/W領域操作コマンドをOPコードを含めて暗号化して(つまりコマンドデータ全体を暗号化して)、SEND命令によりLCM10(内のメディアI/F部13またはPD I/F部12)からPM30側に送る場合について説明したが、これに限るものではない。例えば、図9の形式のコマンド(命令)を用い、コマンドデータ中のOPコードは、暗号化せずに、パラメータ(オペランド)だけを暗号化して、そのパラメータのみが暗号化されたコマンドデータ自体をLCM10からPM30側へ送るようにも構わない。

【0042】この場合の、PM30の動作を簡単に説明する。

【0043】まずコントローラ31は、LCM10からパラメータのみが暗号化された図9の形式の暗号化コマンドを受け取ると、そのコマンド中の暗号化されていないOPコードを解釈し、その解釈結果に応じてPM30の動作(処理の割当て)の最適化を図る。

【0044】OPコードのサイズは1バイトであり、短いデータである。しかし、先の例のように当該OPコードも暗号化されている場合、当該OPコードも復号する必要があり、その復号に一定のオーバヘッドを要する。

【0045】ところが、OPコードの暗号化を行わないならば、LCM10からコマンドを受け取った段階で直ちにOPコードの解釈が実行できるため、上記の如くPM30の動作を最適化することができる。即ちコントローラ31は、OPコードの解釈により、受信コマンドが秘匿R/W領域操作コマンドのうちのREADコマンド、WRITEコマンド、ERASEコマンド、またはCHANGEコマンドのいずれであるかを判定すると、直ちに判定したコマンドの実行シーケンスに入る。そしてコントローラ31は、この実行シーケンスの中で、受

信コマンド中のOPコードを除く部分、つまり暗号化されたパラメータ(オペランド)をコマンド復号部32に渡して、復号を要求する。

【0046】コマンド復号部32は、コントローラ31から渡された暗号化パラメータ(オペランド)を復号する。このコマンド復号部32の復号動作は、復号対象が暗号化パラメータである点を除け、先の暗号化コマンドの復号の場合と同様である。コマンド復号部32は、暗号化パラメータを復号すると、その復号されたパラメータ、つまり平文のパラメータ(オペランド)をコントローラ31に返す。

【0047】コントローラ31は、上記実行シーケンスの中でコマンド復号部32から平文のパラメータを受け取ると、そのパラメータに従って、そのシーケンスに固有の動作、即ち先に解釈したコマンドの指示する動作を行う。

#### 【0048】

【発明の効果】以上詳述したように本発明によれば、デジタル・コンテンツの記録再生に利用される記憶媒体に確保された秘匿領域を操作するための秘匿領域操作コマンドの全体またはパラメータ部分を暗号化して当該記憶媒体に送り、当該記憶媒体ではそれを復号化して実行するようにしたので、秘匿領域操作コマンドの改ざんによるセキュリティの破綻を防ぐことができる。

【0049】また本発明によれば、記憶媒体のメモリ領域上に連続的に確保された秘匿領域と公開領域との境界を特定秘匿領域操作コマンドにより移動して秘匿領域と公開領域のサイズの比率を変更できるだけでなく、少なくとも秘匿領域が縮小変更される場合は、その秘匿領域変更に際してその変更部分のデータが自動的に消去されるため、秘匿されたデータが漏洩するのを防止できる。

#### 【画面の簡単な説明】

【図1】本発明の一実施形態に係るコンテンツ利用管理システムの構成を主として示すブロック図。

【図2】図1中のPM30の構成を示すブロック図。

【図3】図2中のフラッシュメモリ35の記憶領域のメモリマップの一例を示す図。

【図4】OPコードも含めて暗号化される秘匿R/W領域操作コマンドの形式を示す図。

【図5】秘匿R/W領域操作用の暗号化コマンドの送信から実行までの一連の動作を説明するためのフローチャートの一部を示す図。

【図6】秘匿R/W領域操作用の暗号化コマンドの送信から実行までの一連の動作を説明するためのフローチャートの他の一部を示す図。

【図7】秘匿R/W領域操作用の暗号化コマンドの送信から実行までの一連の動作を説明するためのフローチャートの残りを示す図。

【図8】秘匿R/W領域351の開始アドレスがAD1の状態で、CHANGEコマンドによりAD2(但し、

$AD_2 > AD_1$ ）に変更することが指定された場合の、当該CHANGEコマンド実行後のフラッシュメモリ35のメモリマップを示す図。

【図9】パラメータだけが暗号化される秘匿R/W領域操作コマンドの形式を示す図。

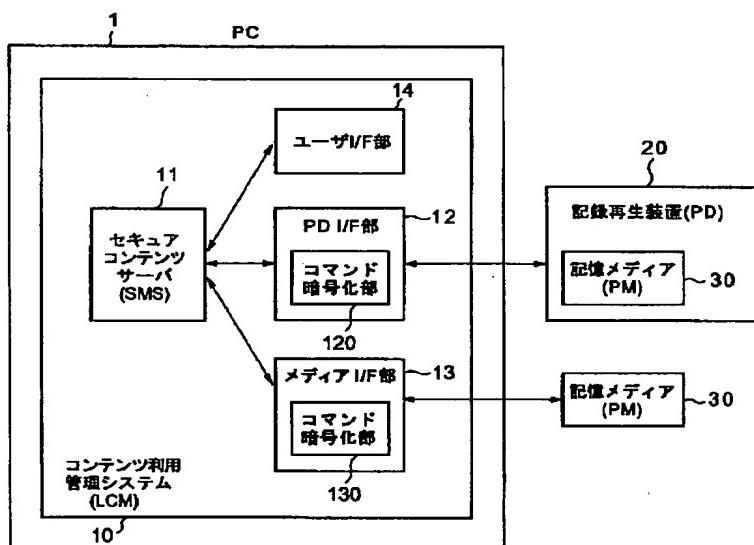
【符号の説明】

- 1 … PC (パーソナルコンピュータ)
- 10 … LCM (コンテンツ利用管理システム、コンテンツ管理装置)
- 11 … セキュア・コンテンツ・サーバ
- 12 … PD I/F部 (送信手段)
- 13 … メディア I/F部 (送信手段)
- 14 … ユーザI/F部
- 10 … LCM (コンテンツ利用管理システム、コンテンツ管理装置)
- 11 … セキュア・コンテンツ・サーバ
- 12 … PD I/F部 (送信手段)
- 13 … メディア I/F部 (送信手段)
- 14 … ユーザI/F部

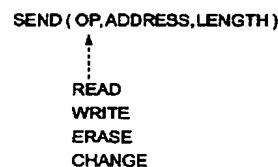
- \* 14 … ユーザI/F部
- 20 … PD (記録再生装置)
- 30 … PM (記憶媒体、記憶メディア)
- 31 … コントローラ
- 32 … コマンド復号部
- 33 … 作業メモリ
- 34 … ROM
- 35 … フラッシュメモリ
- 120, 130 … コマンド暗号化部
- 10 351 … 秘匿R/W領域
- 352 … 公開R/W領域

\*

【図1】



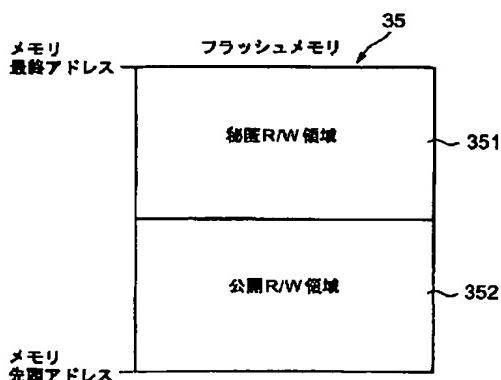
【図4】



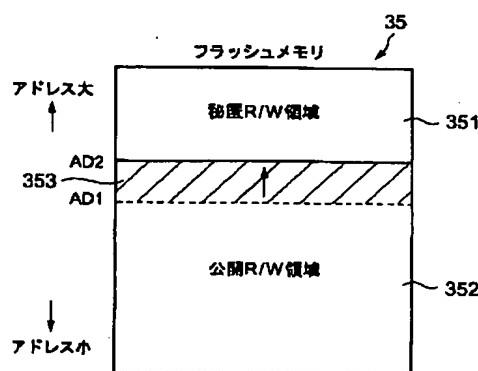
【図9】

- (a) READ (ADDRESS, LENGTH)
- (b) WRITE (ADDRESS, LENGTH)
- (c) ERASE (ADDRESS, LENGTH)
- (d) CHANGE (ADDRESS, LENGTH)

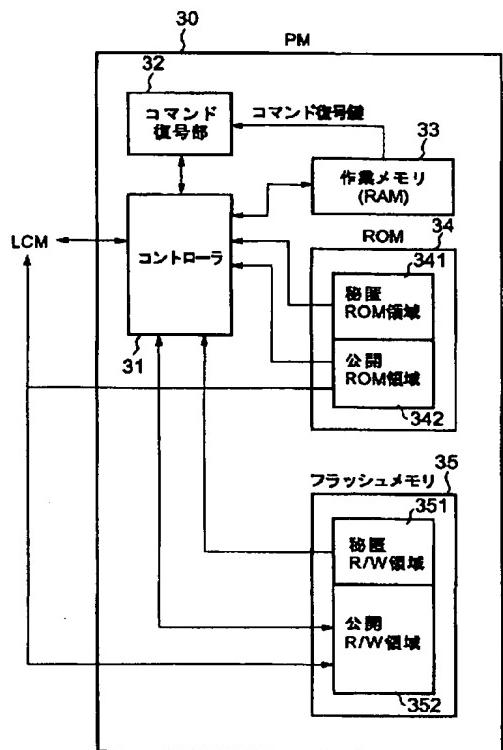
【図3】



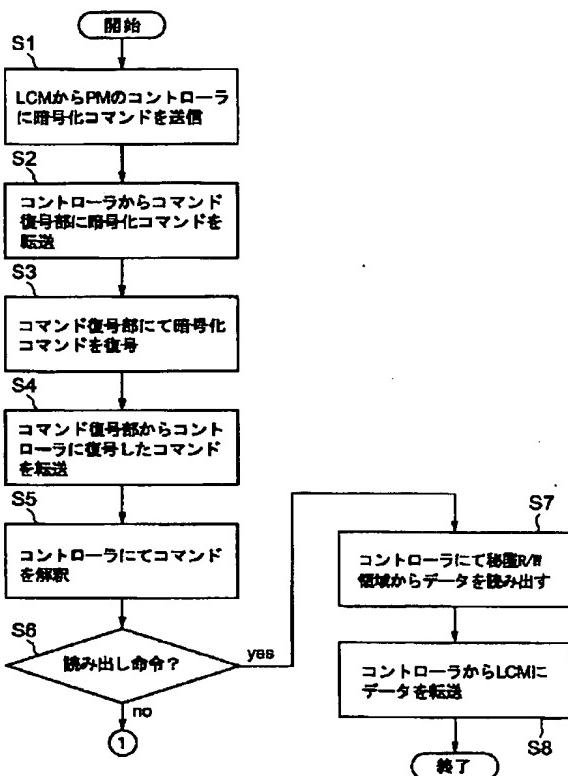
【図8】



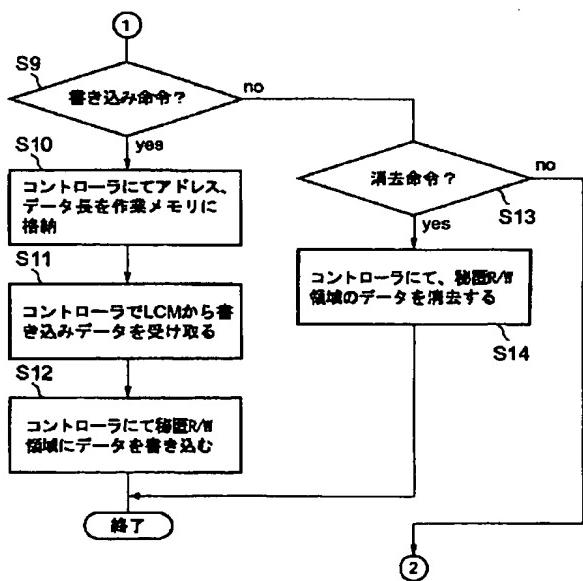
【図2】



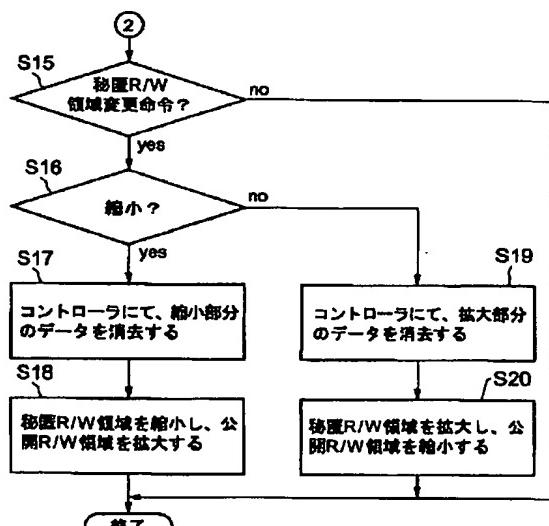
【図5】



【図6】



【図7】



フロントページの続き

F ターム(参考) 5B017 AA07 BA07 BB00 CA14  
5C064 BA07 BB02 BC06 BC16 BC25  
CA14 CB08 CC04  
5J104 AA12 EA10 NA02